STATUS OF THE CLAIMS

Claim 1 (previously presented). A method for carrying out over a network at least one verified, remote electronic transaction between at least one user and at least one merchant by providing to a merchant's server verified user information, which is necessary to complete the verified transaction, the method comprising:

interfacing a machine-readable data structure of the user with a digital, electronic device, wherein the digital electronic device is connected to the network;

providing an access code via the digital electronic device to unlock the machine-readable data structure and to thereby access a database of verifiable user information contained therein; and

providing the verifiable user information to the merchant over a communication link of the network to complete the transaction.

Claim 2 (original). The method of claim 1, wherein verifiable user information is compared with similar user information residing on a verifying server on the network.

Claim 3 (original). The method of claim 1, wherein the machine-readable data structure is selected from the group consisting of an integrated circuit card, a magnetic stripe card, and a bar coded card.

Claim 4 (original). The method of claim 1, wherein at least one merchant is a verifiable merchant.

Claim 5 (previously presented). The method of claim 1, wherein the machine-readable data structure is unlocked by providing an access code through the digital electronic device that matches a previously registered personal security code.

Claim 6 (original). The method of claim 5, wherein the previously registered personal security code is contained in unsecured memory on the machine-readable data structure.

Claim 7 (previously presented). The method of claim 1, wherein a first communication link between said digital electronic device and the merchant's server is established following the unlocking of the machine-readable data structure.

Claim 8 (previously presented). The method of claim 1, wherein the communication link between the digital electronic device and the merchant's server is established through a second communication link from said digital electronic device to a verifying server and then through a third communication link from said verifying server to said merchant's server.

Claim 9 (original). The method of claim 1, wherein verified user information is transmitted to at least one merchant's server to populate at least one merchant's check-out form.

Claim 10 (original). The method of claim 9, wherein verified user information is transmitted to at least one merchant's server to populate at least one merchant's check-out form, following verification of the user's information at a verifying server.

Claim 11 (original). The method of claim 9, wherein said check-out form is populated manually by the user.

Claim 12 (original). The method of claim 9, wherein said check-out form is populated automatically.

Claim 13 (original). The method of claim 1, wherein verified user information is transmitted to at least one merchant's server by automatically populating a

merchant's order database and transaction systems.

Claim 14 (original). The method of claim 13, wherein verified user information is transmitted to at least one merchant's server by automatically populating a merchant's order database and transaction systems following verification of the user's information at a verifying server.

Claim 15 (original). The method of claim 1, wherein the merchant's server contains server-side software to accept direct transmission of verified user information from the machine-readable data structure, without using forms.

Claim 16 (original). The method of claim 1, wherein the network is selected from the group consisting of local area networks, wide area networks, the Internet, and Wireless and Mobile networks.

Claim 17 (original). The method of claim 1, comprising the additional steps of:

providing authorization from the user to complete said verified transaction;

completing said verified transaction;

providing at least one message to the merchant, indicating that said verified transaction comprises a valid, card present equivalent transaction; and

providing at least one message, comprising at least one transaction number, to the user's digital, electronic device to confirm the sale.

Claim 18 (original). A method for providing verified information about at least one user over a network to at least one merchant during at least one electronic transaction, the method comprising the steps:

providing at least one access code provided by the at least one user and unique user information to at least one verifying server, wherein said verifying server is connected to the network;

verifying said access code and unique user information; and

providing verified user information to the at least one merchant.

Claim 19 (original). The method of claim 18, wherein said access code is verified by comparing said access code with a previously registered security code stored on a machine-readable data structure.

Claim 20 (previously presented). The method of claim 19, wherein said access code is verified by presenting said access code through a digital electronic device to the machine-readable data structure.

Claim 21 (original). The method of claim 18, wherein said unique user information is released for verification against similar data stored in at least one database of the at least one verifying server.

Claim 22 (original). The method of claim 21, wherein said unique user information is released for verification against similar data stored in at least one database of the at least one verified server upon verification of the access code.

Claim 23 (original). The method of claim 18, wherein the network is selected from the group consisting of local area networks, wide area networks, the Internet, and Wireless and Mobile networks.

Claim 24 (previously presented). A system enabling a user to complete one or more verified, remote electronic transactions over a network with at least one merchant, said merchant having a server, wherein said verified transactions are completed by providing the merchant's server with verified user information, the system comprising:

a network;

at least one remote verifying server, wherein said remote verifying server is connected to the network and is capable of receiving and verifying verified user information;

at least one remote server maintained by a merchant, wherein the merchant's at least one remote server is connected to the network and is capable of accessing said remote verifying server to receive verified user information therefrom;

at least one remote digital electronic device that is maintained by the user or by a third party, wherein said digital electronic device is connected to the network and is capable of accessing said verifying server to transmit verified user information and said remote server maintained by a merchant to initiate and complete said verified, remote electronic transactions; and

a machine-readable-data structure, having at least one secure memory cache, which interfaces with said digital electronic device.

Claim 25 (original). The system of claim 24, wherein the system further comprises a registered personal security code that is stored in said secure memory cache of said machine-readable data structure.

Claim 26 (original). The system of claim 24, wherein the machine-readable data structure comprises at least one of an integrated circuit card, a magnetic stripe card, or a bar coded card.

Claim 27 (original). The system of claim 26, wherein the integrated circuit card, having a surface, further comprises:

at least one internal microprocessor,

at least one internal semiconductor memory, having a secured first portion for storing verifiable user information and an unsecured second portion, wherein said at least one internal semiconductor memory is controlled by said at least one internal microprocessor; and

at least one mass-storage memory, wherein said at least one mass storage memory is accessible from the surface of the card.

Claim 28 (original). The system of claim 24, wherein said machine-readable data

structure can be unlocked by a security algorithm.

Claim 29 (original). The system of claim 28, wherein said machine-readable data structure can be unlocked by inputting an access code.

Claim 30 (original). The system of claim 29, wherein said machine-readable data structure is unlocked after the access code inputted by the user is verified against a previously registered security code that is stored in said secured first portion of said internal semiconductor memory.

Claim 31 (original). The system of claim 30, wherein said previously registered security code is resident in one or more memory on the machine-readable data structure.

Claim 32 (original). The system of claim 29, wherein said system further comprises software capable of providing verified user information to at least one verifying server for verification upon prior successful access code verification.

Claim 33 (original). The system of claim 24, wherein at least one verifying server provides verified user information to said merchant's server to populate a merchant's check-out form contained therein.

Claim 34 (original). The system of claim 33, wherein said at least one verifying server provides verified user information to said merchant's server by automatically populating an order database and transaction system.

Claim 35 (original). The system of claim 33, wherein said merchant's server contains server-side software to accept direct transmission of the user's machine-readable data, without using forms.

Claim 36 (original). The system of claim 35, wherein said direct transmission of the user's machine readable data is storcd originally on the user's machine-readable data structure.

Claim 37 (original). The system of claim 33, wherein the user manually populates the merchant's check-out form by dragging verified user information from at least one pop-up window and dropping the dragged information into an appropriate location of the merchant's check-out form.